WHAT IS CLAIMED IS:

1. A tamper resistant microprocessor, comprising:

a decryption unit configured to read out an execution code or data of an encrypted program and decrypt the execution code or data by using a prescribed encryption key, according to a decryption request from the cache memory control unit;

a cache memory configured to store the execution code or data decrypted by the decryption unit into one of cache lines provided in the cache memory, each cache line having a secret protection attribute holding section for storing an actual encryption key used in decrypting the execution code or data; and

a cache memory control unit configured to process a reading request for the execution code or data such that, if the execution code or data exists in the cache memory and the execution code or data in the cache memory is decrypted by an identical encryption key as the prescribed encryption key, the execution code or data in the cache memory is read out.

2. The tamper resistant microprocessor of claim 1, further comprising:

a key value register configured to store a desired encryption key to be used in decrypting the execution

code or data, which is updated at each occasion of executing the encrypted program;

wherein the cache memory control unit judges whether the execution code or data in the cache memory is decrypted by an identical encryption key as the prescribed encryption key, by comparing the desired encryption key stored in the key value register and the actual encryption key stored in the secret protection attribute holding section of a cache line for the execution code or data to be executed to see if two encryption keys are identical or not.

3. The tamper resistant microprocessor of claim 2, wherein the cache memory stores data decrypted by the decryption unit, and the cache memory control unit writes a processing result of the data into the cache memory, while storing the desired encryption key stored in the key value register into the secret protection attribute holding section of a cache line for the data.

4. The tamper resistant microprocessor of claim 1, wherein the cache memory stores data decrypted by the decryption unit, and the cache memory control unit encrypts a processing result of the data by using the actual encryption key stored in the secret protection attribute holding section of a cache line for the data,

and writes encrypted data into an external memory device.

5. A data access control method by a cache memory implemented processor, comprising:

reading out an execution code or data or an encrypted program and decrypting the execution code or data by using a prescribed encryption key, according to a decryption request;

storing the execution code or data decrypted by the reading and decrypting step, into one of cache lines provided in a cache memory, each cache line having a secret protection attribute holding section for storing an actual encryption key used in decrypting the execution code or data; and

processing a reading request for the execution code or data such that, if the execution code or data exists in the cache memory and the execution code or data in the cache memory is decrypted by an identical encryption key as the prescribed encryption key, the execution code or data in the cache memory is read out.

6. The data access control method of claim 5, further comprising:

storing a desired encryption key to be used in decrypting the execution code or data, which is updated

at each occasion of executing the encrypted program, into a key value register;

wherein whether the execution code or data in the cache memory is decrypted by an identical encryption key as the prescribed encryption key is judged by comparing the desired encryption key stored in the key value register and the actual encryption key stored in the secret protection attribute holding section of a cache line for the execution code or data to be executed to see if two encryption keys are identical or not.

7. The data access control method of claim 6, wherein the cache memory stores data decrypted by the decryption unit, and the data access control method further comprises writing a processing result of the data into the cache memory, while storing the desired encryption key stored in the key value register into the secret protection attribute holding section of a cache line for the data.

8. The data access control method of claim 5, wherein the cache memory stores data decrypted by the reading and decrypting step, and the data access control method further comprises encrypting a processing result of the data by using the actual encryption key stored in the

secret protection attribute holding section of a cache line for the data, and writing encrypted data into an external memory device.